McRoberts TECHNOLOGIES

MyChild SECURITY FIRST

ASSET WATCH

WANDERWATCH™

STAFF WATCH

Version 6 Applications IT and Networking FAQs

1. What is the receiver and door controller infrastructure?

Wired receivers and door controllers use an RS-485 cabled backbone topology that interfaces to the hospital's network via Integrated Network Manager (INM) device(s). Wireless receivers communicate directly over standard Wi-Fi infrastructure via AMQP/S Protocol.

Wireless Receivers

2. What are the requirements for McRoberts Wireless Receivers?

Powered by three-pronged standard outlets, the McRoberts Wireless Receiver is an ETL-listed receiver with a through-socket for other uses. 15 AMP breakers are requested. It receives tag data via RFID, and it transmits that data to the application server using WPA2-PSK or WPA2-Enterprise authentication over standard 2.4 GHz Wi-Fi. There is a through socket which can be used to power devices using not greater than 8 AMPS, 110 volts AC. Customer must provide an available IP address for each receiver.

3. How is the data transmitted from the McRoberts Wireless Receivers to the application server?

The McRoberts agent, McLink Message Manager, is required to provide gateway communication between the McRoberts Wireless Receivers and the application server. If server is on-premise, the McLink agent can reside on the server hosting the application. If server is cloud-based, Customer must provide an on-premise or VM server to host the McLink agent.

RF Tags

4. How do the tags communicate to the devices and application server?

Tag transmissions have three modes: Tag Locating Message (TLM) beacons, Tag in Communication (TIC) messages, and Tag-to-Door Controller Interchange.

TLM: The tags transmit a signal over a UHF 433 MHz frequency in intervals of once every 16 or 20 seconds, depending on which tag type. The information transmitted consists of the tag ID number and a tag status bit(s). Tag transmissions occur in simplex mode to the receiver(s) in the range of hearing the signal. The receiver listens for tag transmissions at 433 MHz. No acknowledgment (ACK/NAC) is given.

TIC: Tags with a tamper detection mechanism transmit a tamper signal at 433 MHz once tampering has been detected. This signal is picked up by the receiver(s) and sent along to the server. The software interprets the signal and raises an alarm.

Tag to Door Controller Interchange: The door controller generates a low-frequency 307 kHz signal which is used to trigger a tag response when the tag enters the field. The door responds with an acknowledgment at Ultra High Frequency (433 MHz). Once the tag receives this positive response, it transmits the required messaging. This ensures that only valid tag IDs and properly formatted messages can be received. Tag information is then passed to the server.

5. Can the tag-to-device-to-application server create a security vulnerability to the network?

No. Even if an attacker found (sniffed) the proper time slot, the proper sub-channel within the correct frequency, and the proper message air protocol (e.g., OOK, FSK, PSK, QPSK), the only option is to transmit bits resembling the tag ID and status bit(s). Even if the receiver received a “bogus” tag ID string, the only destination is the server database where it would have no system effect. There is no other information capable of transmission to any other device but the server database. There is no network security threat possible from RF to receiver tag transmissions.

Integrated Network Managers and Web Relays

6. When are INMs (Integrated Network Managers) required?

If any wired devices (receivers or door controllers) are part of the system, INM devices are necessary to facilitate communication from RS-485 to TCIP/IP.

7. What are the requirements for the INMs?

If server is on-premise, the McLink agent can reside on the server hosting the application. If server is cloud-based, Customer must provide an on-premise or VM server to host the McLink agent. Each INM device is seen as a virtual COM port on the server that hosts McLink and has an assigned IP address. This allows the server to use TCP/IP to encapsulate the information being sent to and retrieved from the devices on the RS-485 network.

8. Does the system architecture require a Virtual Local Area Network (VLAN) for the INMs to be on the same IP subnet?

The only requirement is that all IP traffic is routed between the client devices, server, and INMs on a low-latency connection with available bandwidth. There is also a data communications requirement that TCP port 773 be open bi-directionally between the server and the INM(s). For on-premise deployments, there is a Structured Query Language (SQL) server requirement that TCP port 1433 be open bi-directionally between the server and SQL server if they are separate. For both cloud and on-premise deployments, the INMs need to be on the same VLAN as the McLink Message Manager server application.

9. When are web relays required?

Dependent on system design.

10. What will be installed in the data/IT/electrical closet(s)?
What are the power and space requirements?

- Power supply(s), each one in a 15.5” x 12” x 4.5” locking storage enclosure
- INM(s) (if applicable), each one in a 7” x 8” locking storage enclosure
- Web Relay(s), each one in a 7” x 8” locking storage enclosure.

These items must be housed in a customer-designated data/IT/electrical closet. McRoberts Technologies strongly recommends that system components be connected to the hospital’s emergency backup power (120 V, 15 AMP). Space requirement is dependent on the number of devices installed in the data/IT/electrical closet.

11. What are the network requirements?

One network drop per INM and one per web relay in the designated data/IT/electrical closet.

Latency Requirements

12. What are the Network Latency Requirements?

Internal Latency Requirement (Perimeter Devices to McLink Agent)

A. Communication Path: Wired Device>INM>Network Switch>McLink Message Manager.
B. The connection between the McLink Message Manager and the INM must not have a packet delay of more than 10ms. Delays greater than 10ms for this segment will trigger a NETWORK IN DEGRADED STATE alarm and critical data may be missed.

Note: Wireless devices are not subject to any internal latency requirements.

External Latency Requirement (Applies Only to Cloud-Based Server)

A. Communication Path: McLink Message Manager>Cloud Application Server.
B. There must be adequate bandwidth to support the traffic.
C. A packet delay of 200 ms *will not negatively impact system functionality*. Delays greater than 500ms could SLIGHTLY negatively impact functionality in that there could be a SLIGHT delay in a door lock releasing when a tag is in bypass mode or when a user enters an authorized PIN code.
D. Packets should never be delayed or be allowed to become discarded while traversing the network. Any disruption in network connectivity will prevent real-time data collection and will impact the system’s availability. This includes the ability to perform tasks and display alarms.

Server

13. Where do the applications reside and how are they accessed?

The applications can run on a cloud-based server hosted by McRoberts Technologies or on an intranet-based server located in a client data center or locally at the facility. They are accessed via a standard web browser using standard HTTP/S Protocol. If cloud-based system is selected

14. What are the requirements for the on-premise server for the applications and/or the McLink agent?

MINIMUM SERVER SPECIFICATIONS:

CPU:	1 CPU 2 CORES
Ram:	8 GB
Hard Drive:	80 GB
Network:	1 GB Full Duplex
IP Addresses:	DHCP Reserved or Static

SOFTWARE REQUIREMENTS:

Microsoft Windows Server 2019 or later operating system
Microsoft .NET CORE 8 Runtime

SOFTWARE RECOMMENDATIONS:

Latest Microsoft Windows Server operating system

NOTES:

- TCP Port 771 open internally to facility
- AMQPS Ports for 5671 and 5672 open for external communications*
- MQTTS Ports for 1883 and 8883 open for external communications*
- Remote Connectivity
    - NinjaRMM/TeamViewer – McRoberts Supplied
    - Bomgar, Securelink, Cisco AnyConnect or similar – Facility Supplied

*For cloud deployment

15. Will this software run on a Virtual Machine (VM)?

Yes. The software is tested using Microsoft Hyper-V and has also been deployed with VMware.

16. What operating systems can the software run on?

The server software applications should be installed on Windows Server 2019 or later. Devices displaying the applications can access them through typical web browsers including Chrome, Edge and Safari.

17. Are there any restrictions on running OS updates or installing patches?

There are no restrictions; however, McRoberts requests to be notified in advance of system maintenance events because restarts can impact the operation of, and notifications seen by, the applications. System maintenance event advance notification should be emailed to TechSupport@McRobertsTech.com. Advance notification of system maintenance events allows McRoberts technicians to monitor the system during the event to minimize any downtime which may be inadvertently created during the update. The connectivity of devices can be monitored and restored quickly, if necessary.

18. What other software components are installed on the system?

- .NET 8 for Server
- Microsoft SQL Server 2022 Express or higher

19. Can we use our existing MS SQL Cluster?

Yes. The applications can run on an existing Microsoft Sequel (SQL) cluster. The installer does not need the System Administrator (SA) password to install the software; however, the installer needs temporary rights to create databases, tables, and stored procedures. The appropriate version of Microsoft SQL Management Studio that is relative to the version of SQL utilized must be installed. The application database can exist on the application server or an SQL server.

20. What are the data backup requirements?

The customer should back up the SQL Server database using whatever method is currently used at the facility. Please note that, by default, the applications are installed with MS SQL Express, which does not include an SQL agent; therefore, it does not support scheduled backups. Customers can upgrade to MS SQL Server using one of their corporate licenses or backup SQL Express manually or via scripts. McTech Version 6 applications do not need to be backed up as they can be entirely re-installed intact as long as a recent database backup is available.

Note: If a cloud-based deployment, the SQL database is snapshotted every day, week and month.

21. Which Antivirus software is approved for this system?

There are no known issues with any vendor’s Antivirus (AV) solution. The following products have been tested: Microsoft Security Essentials (MSE), Norton and McAfee. Regardless of the AV solution used, it is recommended to exclude the following path from AV scanning: C:\McRoberts.

22. Can the server be joined to a Microsoft Domain and Active Directory structure?

Yes. MyChild software can run on either a stand-alone or a domain server; however, the installation of the software must be performed *after* joining a domain.

23. How do McRoberts applications gain access to directories?

McRoberts uses LDAP for on-premise deployments and AzureAD for cloud-based deployments.

24. How are usernames and passwords authenticated?

Usernames and passwords are stored in the application database. When a user tries to authenticate, the application verifies the username and password the user entered against what is stored in the database. If the username and password match what is stored in the database, the application then looks up the user's assigned permissions. In systems where LDAP is utilized, the application sends the authentication request to the LDAP server. If LDAP authenticates, the application looks up the user's assigned permissions.

Cloud-Hosted

25. What are the advantages of selecting the cloud for the application hosting?

- The cloud server is hosted in an AWS redundant data center and managed by McRoberts.
- Amazon Web Services is a trusted partner regarding security.
- Application is updated seamlessly by McRoberts Technologies.
- Elimination of burden of maintaining server.

26. If cloud-hosted, how does McRoberts ensure system uptime?

Version 6 applications are configured and deployed as a highly available service, with auto-scaling and auto-failover, and can be scaled across availability zones to help ensure connectivity and prevent downtime.

27. If cloud-hosted, what will happen if the Wi-Fi goes down and connectivity to the cloud is lost?

Perimeter protection is independent and still functions in the event Wi-Fi goes down; however, the application would not be accessible.

On-Premise Deployment

28. If an on-premise deployment, how is the system supported by McRoberts Technologies?

For on-premise installations, McRoberts Tech Support uses the agent NinjaOne to access the network and server remotely. This agent allows remote auditing, monitoring, patch management and support. Remote support can also be provided through any client provided remote access management platform. On-site support is provided by arrangement via McRoberts Security Technologies Tech Support, which can be reached 24/7/365 at 800-776-7328 or techsupport@mcrobertstech.com.

29. What Wi-Fi systems are you compatible with from a network standpoint? Do you require any special configuration on switches or wireless controllers?

McRoberts Wireless Receivers use any standard 2.4 GHz Wi-Fi for communications only. They do not depend on Wi-Fi access points to determine a tag's location. They require a TCP/IP address and are then configured via an application UI. All wireless receivers need to reside on the same sub-network and be allowed to communicate to the internet for timing and firmware updates.

Support

30. How is the system supported by McRoberts?

McRoberts uses the Ninja agent to access the network and server to monitor the server. This agent provides auditing, monitoring, patch management, and remote support through McRoberts Tech Support. Remote support can also be provided through SecureLink, BeyondTrust (Bomgar), or Cisco AnyConnect. On-site support is provided by arrangement via McRoberts Security Technologies Tech Support, which can be reached 24/7/365 at 800-776-7328.

31. Does McRoberts Technologies offer extended warranty/extended maintenance?

Yes. McRoberts Technologies offer and recommends an extended warranty/extended maintenance/preventive maintenance/annual user refresher training contract.

32. Does McRoberts Technologies offer information/documents on-demand?

Yes. Documents can be found on *help.mctechcloud.com/books/IT*